EXHIBIT A

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Tuulos et al.	
U.S. Pat. No.:	7,933,211	Attorney Docket No.: 35548-0132IP1
Issue Date:	April 26, 2011	
Appl. Serial No.:	11/737,287	
Filing Date:	April 19, 2007	
Title:	METHOD AND SYSTEM FOR PROVIDING PRIORITIZED FAILURE ANNOUNCEMENTS	

Mail Stop Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES PATENT NO. 7,933,211 PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42

TABLE OF CONTENTS

EXHIBITS

EX1001	U.S. Patent No. 7,933,211 to Tuulos et al. ("the '211 patent")
EX1002	Prosecution History of the '211 Patent (Serial No. 11/737,287)
EX1003	Declaration of Nathaniel J. Davis IV, Ph.D.
EX1004	U.S. Patent No. 5,461,628 ("Nakamura")
EX1005	International Telecommunication Union Recommendation X.733, DATA COMMUNICATION NETWORKS: INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – SYSTEMS MANAGEMENT: ALARM REPORTING FUNCTION ("X.733")
EX1006	U.S. Patent Application Publication No. 2006/0258348 ("Rajala")
EX1007	U.S. Patent No. 6,769,024 ("Natarajan")
EX1008	English Translation of Japanese Patent Application Publication H5-252160 ("Okada")
EX1009	U.S. Patent No. 6,167,025 ("Hsing")
EX1010	U.S. Patent No. 6,122,759 ("Ayanoglu")
EX1011	U.S. Patent Application Publication No. 2007/0263856 ("Parsa")
EX1012	Complaint filed in *WSOU Investments LLC v. Huawei Technologies Co., Ltd., et al.*, Case No. 6:20-cv-00893 (W.D. Tex.)
EX1013	Japanese Patent Application Publication H5-252160
EX1014	Declaration of Jacob Munford
EX1015	English Translation of Kawamura et al., Self-Healing Techniques Utilizing the Virtual Path Concept for ATM Networks (IEICE Transactions B-1, Vol. J74-B-I, No. 7, pp. 537-546) (July 1991) ("Kawamura")

EX1016 U.S. Patent No. 6,820,213 ("Somers")

EX1017 U.S. Patent Application Publication No. 2008/0074247 ("Plantamura")

EX1018 U.S. Patent No. 7,004,625 ("Egidio")

EX1019 3GPP TS 32.111-1 V6.0.1, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Fault Management; Part 1: 3G fault management requirement (Release 6) ("TS32.111")

EX1020 Aomar Osmani et al., Model-Based Diagnosis for Fault Management in ATM Networks (IEEE 1999) ("Osmani")

EX1021-1099 Reserved

EX1100 Complaints filed in *WSOU Investments LLC v. Huawei Technologies Co., Ltd., et al.*, Case Nos. 6:20-cv-00889–00893, 6:20-cv-00916–00917 (W.D. Tx.)

EX1101 Scheduling Order (Document 29), *WSOU Investments LLC v. Huawei Technologies Co., Ltd., et al.*, Case Nos. 6:20-cv-00889, 6:20-cv-00891-00893, 6:20-cv-00916-00917 (W.D. Tx.)

EX1102 Huawei's Stipulation served in *WSOU Investments LLC v. Huawei Technologies Co., Ltd., et al.*, Case Nos. 6:20-cv-00889, 6:20-cv-00891-00893, 6:20-cv-00916-00917 (W.D. Tx.)

CLAIM LISTING

Claim Element	Claim Language
[1.P]	A method comprising:
[1.1]	defining at least two priority indicators for a fault correction;
[1.2]	determining at a network element of a communication network management system a fault correction priority based on said at least two priority indicators, in response to a detection of said fault condition or failure at said network element; and
[1.3]	determining, at said network element, to transmit an announcement notification to a network management function, said announcement notification indicating said detected fault condition or failure and comprising an information about said determined fault correction priority.
[2]	A method according to claim 1, wherein said at least two priority indicators are selected from a perceived severity of said detected fault condition or failure, a criticality of said network element, a performance of said network element, and at least one predetermined environmental condition.
[3]	A method according to claim 2, wherein said at least one predetermined environmental condition is derived from a detection of at least one of a temperature, humidity, radio frequency noise level, or water level.
[4]	A method according to claim 2, wherein said severity is determined in accordance with a predetermined standard.
[5]	A method according to claim 2, wherein said criticality of said network element is determined in dependence on at least one of a location, role and compensation option of said network element.
[6]	A method according to claim 2, wherein said performance of said network element is determined by comparing traffic load prior to and during said detected fault condition or failure.

Claim Element	**Claim Language**
[7]	A method according to claim 1, wherein said announcement notification is an alarm notification.
[8.P]	A system comprising:
[8.1.i]	a determination unit configured to,
[8.1.ii]	determine, at a network element of a communication network management system, a fault correction priority based on at least two priority indicators, in response to a detection of a fault condition or failure at said network element, and
[8.1.iii]	determine, at said network element, to transmit an announcement notification to a network management function, said announcement notification indicating said detected fault condition or failure and comprising an information about said determined fault correction priority; and
[8.2]	a management activity control unit configured to prioritize management actions of said network management function based on said information about said determined fault correction priority.
[9]	A system according to claim 8, wherein said determination unit is further configured to determine as said priority indicators a perceived severity of said detected fault condition or failure, a criticality of said network element, a performance of said network element, and at least one predetermined environmental condition.
[10]	A system according to claim 9, wherein said at least one predetermined environmental condition is derived from a detection of at least one of a temperature, humidity, radio frequency noise level, and water level.
[11]	A system according to claim 9, wherein said severity is determined in accordance with a predetermined standard.
[12]	A system according to claim 9, wherein said criticality of said network element is determined in dependence on at least one of a location, role and compensation option of said network element.

Claim Element	**Claim Language**
[13]	A system according to claim 9, wherein said performance of said network element is determined by comparing traffic load prior to and during said detected fault condition or failure.
[14]	A system according to claim 9, wherein said announcement notification is an alarm notification.
[15.P]	A network element of a communication network management system comprising:
[15.1]	a determination unit configured to determine a fault correction priority based on at least two priority indicators, in response to a detection of a fault condition or failure at a network element; and
[15.2]	a message generation unit configured to add an information about said determined fault correction priority to an announcement notification,
[15.3]	wherein said determination unit is further configured to determine to transmit said announcement notification to a network management function.
[16]	A network element according to claim 15, wherein said determination unit is further configured to determine as said priority indicators a perceived severity of said detected fault condition or failure, a criticality of said network element, a performance of said network element, and at least one predetermined environmental condition.
[17]	A network element according to claim 16, wherein said at least one predetermined environmental condition is derived from a detection of at least one of a temperature, humidity, radio frequency noise level, and water level.
[18]	A network element according to claim 16, wherein said severity is determined in accordance with a predetermined standard.
[19]	A network element according to claim 16, wherein said criticality of said network element is determined in dependence on at least one of a location, role and compensation option of said network element.

Claim Element	**Claim Language**
[20]	A network element according to claim 16, wherein said performance of said network element is determined by comparing traffic load prior to and during said detected fault condition or failure.
[21]	A network element according to claim 15, wherein said announcement notification is an alarm notification.
[22]	A non-transitory computer readable storage medium comprising computer program code, said computer readable storage medium and said computer program code configured to, with one or more processors, cause an apparatus to at least perform the method of claim 1.

Huawei Technologies Co., Ltd. ("Huawei" or "Petitioner") petitions for *Inter Partes* Review ("IPR") of claims 1-22 of U.S. Patent No. 7,933,211 ("the '211 patent").

I. MANDATORY NOTICES—37 C.F.R § 42.8(a)(1)

A. Real Party-In-Interest—37 C.F.R. § 42.8(b)(1)

Huawei Technologies Co., Ltd.; Huawei Device USA, Inc.; Huawei Technologies USA Inc.; Huawei Investment & Holding Co., Ltd.; Huawei Device (Shenzhen) Co., Ltd.; Huawei Device Co., Ltd.; Huawei Tech. Investment Co., Ltd.; and Huawei Device (Hong Kong) Co., Ltd. are the real parties-in-interest. No other parties had access to or control over this Petition, and no other parties funded this Petition.

B. Related Matters—37 C.F.R. § 42.8(b)(2)

WSOU Investments, LLC d/b/a Brazos Licensing and Development ("WSOU")—the alleged Patent Owner—filed on September 29, 2020 a complaint asserting the '211 patent against Huawei Technologies Co., Ltd. and Huawei Technologies USA Inc. in the U.S. District Court for the Western District of Texas (Case No. 6:20-cv-00893). The complaint was one of six patent lawsuits filed by WSOU against Huawei between September 29, 2020 and October 2, 2020:

Asserted Patent No.	Civil Case No. (W.D. Tex.)
6,704,304	6-20-cv-00889
7,406,260	6-20-cv-00891
7,460,658	6-20-cv-00892
7,933,211	6-20-cv-00893
7,406,074	6-20-cv-00916
7,423,962	6-20-cv-00917

None of the six asserted patents is related to another.

Petitioner is not aware of any disclaimers or reexamination certificates addressing the ’211 patent.

C. Lead And Back-Up Counsel—37 C.F.R. § 42.8(b)(3)

Huawei provides the following designation of counsel.

Lead Counsel	Backup counsel
Michael T. Hawkins, Reg. No. 57,867 Fish & Richardson P.C. 3200 RBC Plaza 60 South Sixth Street Minneapolis, MN 55402 Tel: 612-337-2569 hawkins@fr.com	Nicholas Stephens, Reg. No. 74,320 Tel: 612-766-2018 / nstephens@fr.com Kim Leung, Reg. No. 64,399 Tel: 858-6784713 / leung@fr.com Kenneth Hoover, Reg. No. 68,116 Tel: 512-226-8117 / hoover@fr.com Sangki Park, Reg. No. 77,261 Tel: 612-638-5763 / spark@fr.com Rishi Gupta, Reg. No. 64,768 Tel: 214-292-4056 / rgupta@fr.com Patrick J. Bisenius, Reg. No. 63,893 Tel: 612-766-2048 / bisenius@fr.com

	Terry J. Stalford, Reg. No. 39,522 Tel: (214) 292-4088 / stalford@fr.com

D. Service Information

Please address all correspondence and service to the address listed above. Huawei consents to electronic service by email at 35548-0132IP1@fr.com (referencing No. 35548-0132IP1 and cc'ing PTABInbound@fr.com and hawkins@fr.com).

II. PAYMENT OF FEES

Huawei authorizes the Office to charge Deposit Account No. 06-1050 for the fee set in 37 C.F.R. § 42.15(a) and further authorizes payment for any additional fees to be charged to this Deposit Account.

III. REQUIREMENTS FOR IPR

A. Standing

Huawei certifies that the '211 patent is available for IPR and that Huawei is not estopped from requesting IPR.

B. Challenge and Relief Requested

Huawei requests IPR of claims 1-22 of the '211 patent on the grounds listed below. A declaration from Dr. Nathaniel Davis (EX1003) supports this Petition.

Ground	Claims	§103 Combination
1A	1-2, 6-7	Okada in view of Rajala
1B	1-2, 5, 8-9, 12-16, 19-22	Okada in view of Rajala and Hsing
1C	2, 4, 9, 11, 16, 18	Okada in view of Rajala, Hsing, and X.733
1D	2-3, 9-10, 16-17	Okada in view of Rajala, Hsing, X.733, Ayanoglu, and Parsa
2A	1-21	Nakamura in view of X.733 and Rajala
2B	22	Nakamura in view of X.733, Rajala, and Natarajan

The ’211 patent does not make a claim of priority. For purposes of this Petition, Huawei treats the April 19, 2007 filing date of the ’211 patent as the Critical Date for evaluating prior art status:

Reference	Filed	Published	Status
Nakamura (EX1004)	06/16/1994	10/24/1995	§§102(a)-(b), (e)
X.733 (EX1005)	---	1992	§§102(a)-(b)
Rajala (EX1006)	07/18/2006	11/16/2006	§§102(a), (e)
Natarajan (EX1007)	02/05/2003	07/27/2004	§§102(a)-(b), (e)
Okada (EX1008)	---	09/28/1993	§§102(a)-(b)
Hsing (EX1009)	09/05/1997	12/26/2000	§§102(a)-(b), (e)
Ayanoglu (EX1010)	10/10/1995	09/19/2000	§§102(a)-(b), (e)
Parsa (EX1011)	08/30/2006	11/15/2007	§102(e)

None of the references were formally cited or applied in a rejection during

prosecution. X.733 is discussed in the specification of the '211 patent.

IV. THE '211 PATENT

A. Brief Description

The '211 patent generally describes "[a]n approach for announcing a fault condition or failure in a network system." EX1001, Abstract; EX1003, ¶¶32-36. The '211 patent notes explains that "[f]or a network operator, managing the network, it is difficult to prioritize corrective actions for failures due to huge amount of alarms (which can be thousands per day) as well as the amount of network entity instances to which the alarms relate to." *Id.*, 1:66-2:4; *see also id.*, 2:19-32, FIG. 6. The '211 patent purports to address this problem by supplementing fault announcement notifications (e.g., alarms) with "additional information about the priority for fault correction" as calculated locally at the network element. *Id.*, 4:59-5:10; *see also id.* 5:26-36, FIGS. 1-4. "By determining and adding the fault correction priority already at the source network element, operator and/or management activities can be optimized" and "[t]he need for transmitting data (which affects action prioritization) to the network management function and then post-processing that data is avoided." *Id.*, 3:28-38.

Figure 2 depicts a network element having a determination unit 44 configured to generate a fault correction priority based on priority indicators including site location L, traffic throughput TT, and other diagnostic data DD, according to a

preferred embodiment:

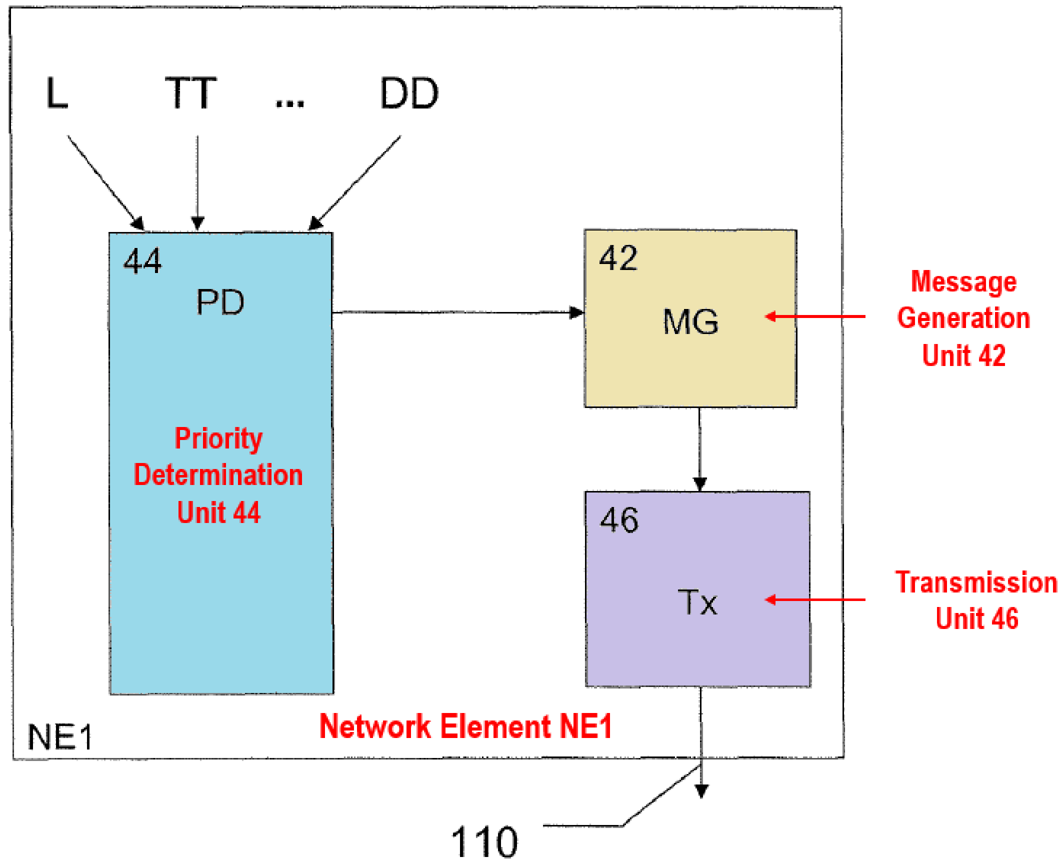


Fig. 2

EX1001, FIG. 2 (annotated).

B. Summary of the Prosecution History

In a first office action, independent claims 1, 8, and 15 were rejected under 35 U.S.C. §102 over Somers (EX1016). EX1002, 101-109. The applicant's response disputed that Somers' teaching of "relative CPU priorities" corresponded to a "fault correction priority," and the applicant argued that Somers' determination of priorities "if [] diagnostic procedures fail to detect problems" did not meet the claim

language that required determination of a fault correction priority "in response to a detection of said fault condition or failure at said network element." EX1002, 85-98.

The next office action rejected the claims under 35 U.S.C. §102 over Plantamura (EX1017). EX1002, 77-83. The applicant eventually appealed this rejection, and in an appeal brief, sought to distinguish Plantamura by emphasizing that the claims require determination of the fault correction priority "at a network element" and "in response to a detection of said fault condition or failure at said network element." EX1002, 35-36; *see also id.*, 28-43, 54-62, 63-73, 77-83.

Following submission of the appeal brief, the applicant agreed to an examiner's amendment in which the independent claims were amended to clarify that the "network element" is of "a <u>communication</u> network <u>management</u> system." *Id.*, 19-24. The examiner then mailed a notice of allowance, and provided reasons for allowance that indicated the "prior art made of record fails to teach or fairly suggest in combination" the various features recited in claims 1, 8, 15. *Id.* However, the record indicates that the examiner had not considered the prior art combinations described in Grounds 1(A)-2(B) of this Petition. If these grounds had been considered, the application would not have been allowed. EX1003, ¶¶37-41.

V. LEVEL OF ORDINARY SKILL

A person of ordinary skill in the art at the time of the '211 patent (a

"POSITA") would have had a Master's degree in computer science, computer engineering, or a related field, with 3-5 years of experience in data communication networks. EX1003, ¶¶27-31. Such experience could be obtained through research and study in a graduate program or through comparable exposure to research literature through industry employment working in the field of network management, and additional years of experience could substitute for the advanced-level degree. *Id.*

VI. CLAIM CONSTRUCTION

All claim terms should be construed according to the *Phillips* standard. *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005); 37 C.F.R. §42.100. In the Related Litigation, a *Markman* hearing is scheduled for August 12, 2021. EX1101, 3. For purposes of Grounds 1(A)-2(B) in this Petition, no construction is necessary due to the noticeable overlap between the preferred embodiment of the '211 patent and the predictable results of the obviousness combinations detailed below. *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011).

VII. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. GROUND 1A: OKADA IN VIEW OF RAJALA (Claims 1-2, 6-7)

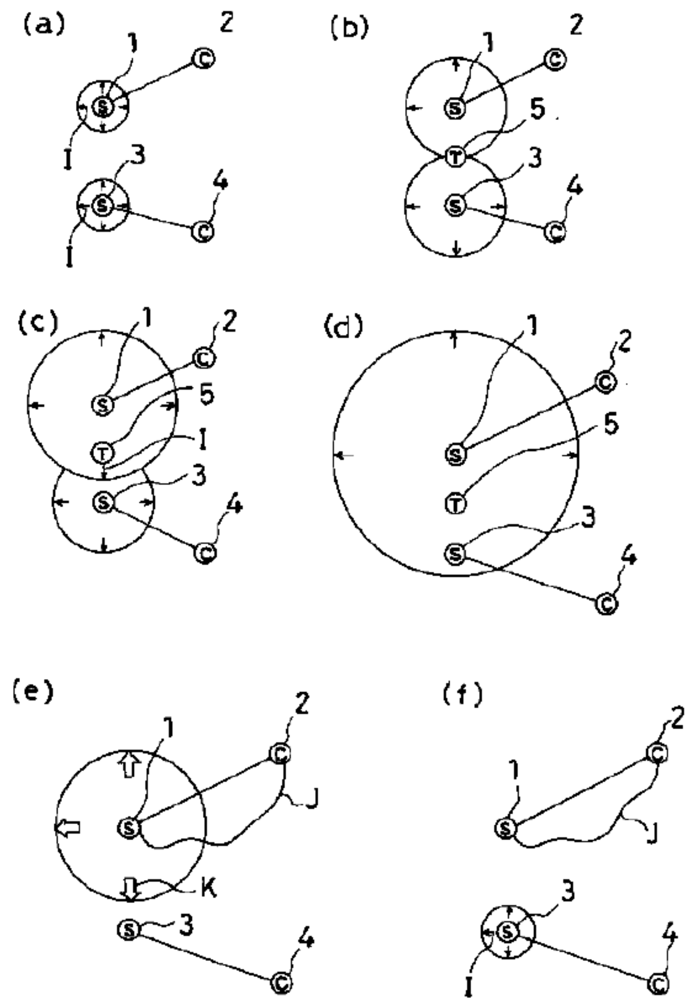
1. Overview of Okada

Okada describes a "method for fault recovery" in a communications network "when multiple faults occur." EX1008, [0001], FIG. 1; EX1003, ¶¶54-58.

"Conventionally a 'self-healing scheme has been proposed as a method for recovery when a fault has occurred," and in such a scheme, "when a fault occurs, nodes on both ends of the fault autonomously, and in a decentralized manner, set up a bypass circuit to achieve recovery." EX1008, [0003]; *see also* [0002]-[0009] & FIGS. 2-3 (description of purportedly "conventional" self-healing schemes—of which some operations are also used in Okada's method); EX1008, ¶¶55-57. Sometimes, multiple faults occur in the network simultaneously, and the network nodes must prioritize the recovery processes for each fault. *Id.*, [0004].

Okada's fault recovery method prioritizes faults based on "priority levels" recorded in fault recovery messages, where the priority level is determined based on the "importance" and "capacity" of the failed link. *Id.*, [Claim 1], [0005], [0012]-[0020], FIG. 1.

[FIG. 1]



EX1008, FIG. 1.

2. Overview of Rajala

Rajala "relates to monitoring and maintaining a network in telecommunications networks which comprise a large number of network elements." EX1006, [0001], [0005]-[0006]; EX1003, ¶¶59-61. As with Nakamura and the '211 patent, Rajala recognized that "[a] problem in [] existing applications is that the vast number of alarms, many being generated by the same fault, hinders the timely and

efficient monitoring of faults." *Id.*, [0006]; *generally id.*, [0001]-[0014].

3. Analysis of Okada in view of Rajala

Element [1.P]

To the extent the preamble is a limitation, Okada discloses the recited method. EX1008, [Claim 1] ("fault recovery method"), [0001] (same), [0003], [0013], [0015], FIG. 1; EX1003, ¶76.

Element [1.1]

Okada describes parameters indicative of a "capacity" and an "importance" of a failed link. EX1008, [Claim 1], [0013]-[0014], [0022]. In Okada's fault recovery process, a SENDER node calculates recovery priority levels for a failed link based on the "capacity" and "importance" parameters. *Id.*, [0005] ("[t]he nodes 41 and 43 that are the SENDER nodes calculate recovery priority levels from the capacity values, importance levels, and the like, of the failed links, and record the recovery priority levels in the fault recovery messages"); *see also id.*, cl. 1, [0013]-[0014], [0020], [0022] (same); EX1003, ¶¶77-78. The priority evaluating node uses the priority levels that were calculated based on the respective capacity and importance attributes of the failed links to identify which of the links has the highest priority for fault correction/recovery. *Id.*, [0015] ("The node 5 that is the priority evaluating node evaluates, based on the recovery priority levels recorded in the fault recovery messages I, which of the faults is to be restored first[] …"); *see also id.*,

[Claim 1], [0013]-[0019], [0022], FIG. 1. The "capacity" and "importance" parameters thus define "at least two priority indicators for a fault correction" (e.g., correction of a fault at the SENDER node by restoration around the failed link) as recited in claim 1. EX1003, ¶¶77-79.

Element [1.2]

Okada discloses a SENDER node ("network element") that determines a recovery priority level ("fault correction priority") of a failed link based on the "capacity" and "importance" of the link ("based on said at least two priority indicators"). EX1008, [Claim 1] ("priority levels … calculated through the capacities and importance levels of the failed links"); *see also id.*, [0005] ("SENDER nodes calculate recovery priority levels"), [0013]-[0014], [0022] (same); *supra*, Element [1.1]; EX1003, ¶¶80-83.

Further, the SENDER node determines the recovery priority level in response to a detection of a fault condition or failure at the SENDER node. EX1003, ¶¶80-81. For example, paragraph [0005] confirms that the SENDER nodes calculate the recovery priority levels. EX1008, [0005]. Since Okada's nodes only function as a SENDER node in a self-healing process that is initiated in response to detection of a failed link, the recovery priority level is not predetermined, but is instead determined in response to detection of the failed link. EX1008, [0003] ("when a fault A occurs, one of the nodes 31 of the failed terminal becomes a SENDER

node”), [0005], [0013]-[0015], [0022], FIG. 1.

To the extent Element [1.2] requires that the fault condition or failure occurs at the network element itself, Okada also discloses this feature. EX1003, ¶81. Although Okada refers to a “failed link,” a POSITA would have recognized that the link failure (e.g., damage to the physical link medium) also manifests in fault conditions at the respective nodes on either end of the link (including the SENDER node (“network element”)). EX1003, ¶81. For example, a link failure also results in a fault condition or failure in which the SENDER and CHOOSER nodes are unable to fulfill their functions in communicating data through the link or maintaining communication through the nodes. *Id.* EX1008, [Claim 1] (“routing around a failed transmission path through forming a bypass circuit when a fault has occurred in a network”). Indeed, the ’211 patent similarly describes embodiments in which the root cause of a fault condition or failure is *external* to the network element itself—demonstrating that a root failure may manifest in additional fault conditions or failures at one or more network elements. *Cf.* EX1001, 1:56-62 (“A root cause for a fault state can be … a radical change in the environment, like rain or fog hindering signal transmission to a receiver, … external RF noise hindering signal receipt at a receiver, …, etc.”); EX1003, ¶ 81(citing EX1005, EX1019, EX1020).

Okada further discloses how the nodes form a communications network that

manages faults through self-healing routines. EX1008, [0013]-[0015], FIG. 1. Okada's restoration techniques were intended to improve upon the algorithm disclosed in Kawamura (EX1015), thereby suggesting applicability of Okada's technique to an ATM network. EX1008, [0005]. To the extent Okada does not express refer to the SENDER node ("network element") located within a "communication network management system," as recited in claim 1, this feature would have been predictable in the resulting Okada-Rajala combination for the reasons described in further detail below (Element [1.3]). EX1003, ¶¶82-83.

Element [1.3]

Okada's SENDER node ("network element") determines to transmit a fault recovery message to announce/notify the neighboring and nearby nodes of the failed link. EX1008, [0013] ("one of the nodes of a failed terminal sending fault recovery messages to neighboring nodes"), [0015] ("SENDER nodes, which send fault recovery messages I to neighboring nodes"), FIG. 1; *see also id.*, [0002], FIG. 2. The neighboring/nearby nodes function to facilitate network management by participating in the process that establishes a bypass circuit around the failed link. *Id.*; EX1003, ¶¶84-91. For example, when multiple faults occur, a nearby/neighboring node that receives multiple fault recovery messages becomes a "priority evaluating node" that assesses the relative priorities of fault recovery messages corresponding to each of the multiple faults. EX1008, [0014]-[0016],

[Claim 1], FIG. 2. The fault recovery message indicates the detected fault condition or failure stemming from the failed link and includes a value indicative of the link's recovery priority level ("fault correction priority"). EX1008, [0005], [0015], [0020], Cl. 1, Cover Page [Structure] ("recovery priority level values, recorded in the fault recovery messages"). Okada's neighboring/nearby nodes such as the priority evaluating node thus provide a first alternative mapping for the recited "network management function."

Even if Okada was viewed as not expressly disclosing Element [1.3], the elements also would have been achieved in a second alternative mapping by the predictable combination of Okada in view of Rajala—further confirming the conventional nature of the claimed "network management function." EX1003, ¶¶86-87. Rajala describes how network fault management traditionally involves a "centralized network management system (NMS)" collecting "alarms and other network management information" from network elements "in a centralized manner." EX1006, [0005]; *generally id.*, [0001]-[0006]; *supra*, Section VII.A.2. The NMS and network monitoring personnel can then "monitor[] alarms, evaluat[e] their importance and effects and, accordingly, [] initiat[e] repairs." EX1006, [0006]; *see also id.*, [0028] ("any network management system"), [0033] ("network elements send alarms to the network management system NMS in real time or in near-real time"), [0034], FIG. 1. It would have been obvious to a POSITA to

implement Okada in accordance with Rajala's suggestion (e.g., sending fault management alarms to a centralized NMS) such that the SENDER node would not only broadcast a fault recovery message to neighboring/nearby nodes to establish a bypass circuit around a failed link, but would also determine to transmit (and would transmit) an alarm ("announcement notification") to a centralized NMS ("network management function") indicating the fault condition or failure stemming from the failed link. EX1003, ¶¶87-88. The alarm notification would also predictably include an indication of the relative priority level of the failed link ("information about said determined fault correction priority") calculated by the SENDER node, as discussed in detail below.[1] *Id.*

Multiple reasons would have motivated a POSITA to apply Rajala's

[1] In this predictable combination, the Okada-Rajala system would have also achieved the "communication network management system" as recited in Element [1.2]. EX1003, ¶82. For example, the NMS in Okada-Rajala would have, according to Rajala's teachings, provided centralized management of the communications network elements (e.g., ATM switches) disclosed in Okada. *Id.* The NMS and network nodes would have collectively formed a "communication network management system." *Id.*

suggestions to Okada in this manner. EX1003, ¶88. **First**, by reporting an alarm concerning the failed link to a centralized NMS, network operators would be notified of the failure so that repairs could be scheduled or dispatched to address the underlying problem (e.g., to repair or replace damaged cable or network equipment in the failed link). EX1003, ¶89. While Okada's restoration techniques can establish a "bypass circuit," the root cause of the failure (e.g., a physical condition) will often still require repair, and reporting the fault to the centralized NMS would bring the problem to the attention of appropriate authorities.

Second, providing the calculated priority level of the link in the alarm that the SENDER node transmits to the centralized NMS would have been obvious based on Okada's and Rajala's similar teachings about the importance of prioritizing fault corrections in a network. EX1003, ¶90. Okada calculates the priority level in the first instance to ensure that bypass circuits are first established for higher priority links before lower priority links. EX1008, Cl. 1, [0005], [0013]-[0015], [0022]. Rajala also emphasizes the need for fault corrections to be addressed according to their relative priorities, and discloses how the centralized NMS aids network administrators in prioritizing fault corrections. EX1006, [0006] ("prioritize faults and focus the repairs efficiently on the faulty network elements"), [0013]-[0016]. And since the SENDER node already calculates the relative priority level for purposes of the self-healing scheme, it would have been obvious to include

information indicating the relative priority (e.g., a fault correction priority) in the alarm sent to the centralized NMS both to inform the NMS and network administrators of the priority level and to avoid need for duplicate computations of the priority level at the centralized NMS after it has already been determined locally at the SENDER node. EX1003, ¶¶90-91 (citing EX1020).

Claim [2]

Okada's "capacity" parameter indicates a "perceived severity of [a] detected fault condition or failure" since the severity of a link failure is proportionate to the capacity of the link—especially where more connections/bandwidth are impacted by failure of a link with higher capacity. EX1003, ¶¶92-94; *supra* Elements [1.1]-[1.2]; EX1008, [0005]. Link "capacity" can also indicate a "criticality" of the SENDER node ("network element") since a SENDER node that switches higher traffic loads from a higher capacity link is more critical to network performance in handling more network traffic than a node that switches lower traffic loads from a lower capacity link. *Id.* Link "capacity" can also indicate a "performance" of the SENDER node since a node that switches higher traffic loads would have a higher performance level than a node that switches less traffic. EX1003, ¶¶92-94. Okada's "importance" parameter is likewise indicative of a "severity" of the link failure and/or a "criticality" of the network element. *Id.* For instance, failure of a more "important" link will more severely impact network performance standards. *Id.* Likewise,

SENDER nodes serving more important links would be deemed more critical to the network than nodes serving less important links. *Id.*

Rajala also discloses that "[t]he importance of the alarms mainly depends on two factors: 1) the effect of the alarm on the performance of the network element, and 2) the importance of the network element." EX1006, [0006]. Based on this teaching, it would have been obvious to further modify Okada so that calculated priority levels are determined based on factors indicative of the effect of the fault on the "performance" of the network element and the "importance" or "criticality" of the network element as suggested by Rajala. EX1003, ¶¶95-96. A POSITA would have implemented the modification so that NMS and priority evaluating nodes would address failures having a greater impact on performance lesser impact failures. EX1003, ¶97. Additionally, prioritizing based on the importance or criticality of the network element is already suggested by Okada's "importance" parameter, and would promote more effective network management by restoring links utilized by more importance nodes before those utilized by less important nodes. EX1003, ¶98. Okada also indicates that additional or different factors can be used to determine priority levels. EX1008, [0005] ("capacity values, importance levels, ***and the like***"); EX1003, ¶99.

Claim [6]

Rajala prioritizes repairs of network elements based on metrics that indicate

how much current traffic conditions during a fault condition or failure deviate from normal traffic conditions prior to the fault condition or failure. EX1006, [0037] ("calculate a normal value, a current value and/or a relative or an absolute deviation from the normal value"), [0012]-[0013], [0038], [0043] ("amount of traffic"), [0044], FIG. 6; EX1003, ¶¶100-102. Calculating the deviation between the normal and current traffic loads involves "comparing" the traffic load prior to and during a detected fault condition since "deviation" is a measure of how much the current load has departed from the normal load. *Id.*

A POSITA would have found it obvious to implement the Okada-Rajala system in view of Rajala's suggestion such that the priority level of the failure is calculated further based on the deviation of a current traffic load at the SENDER node after the detected fault to a normal load at the SENDER node before the fault in accordance with Rajala's teachings here. EX1003, ¶101-102. A POSITA would have modified Okada in this manner since, as expressly discussed in Rajala, measuring deviation in traffic load is important in assessing the significance/degree of a fault condition, and in prioritizing repairs. EX1006, [0012]-[0013]; EX1003, ¶¶100-102.

Claim [7]

As discussed above (Element [1.3]), the SENDER node sends an "alarm" notification to the centralized NMS according to the teachings of Okada in view of

Rajala. EX1006, [0003], [0007]; EX1008, [0013]-[0015]; EX1003, ¶103.

B. GROUND 1B: OKADA IN VIEW OF RAJALA AND HSING (Claims 1-2, 5, 8-9, 12-16, 19-22)

1. Overview of Hsing

Hsing describes "communication networks and, more particularly, [] methods and apparatus for restoring connections in networks including, e.g., networks which support asynchronous transfer mode (ATM) operation." EX1009, 1:13-17; EX1003, ¶¶62-64.

2. Analysis of Okada in view of Rajala and Hsing

Element [1.P]

Supra, Element [1.P] (Section VII.A.3); EX1003, ¶104.

Element [1.1]

Supra, Element [1.1] (Section VII.A.3); EX1003, ¶105.

Element [1.2]

Hsing describes ATM networks like Okada's, and explains that "[a] network fault condition such as the failure of a link between nodes or the failure of a node in the network can result in the interruption of the transfer of data through the network." EX1009, 2:45-48; EX1003, ¶106. Hsing also discloses processes for restoring connections in an ATM network that stem from "link or node failures." *Id.*, 4:21-40.

To the extent Element [1.2] requires that the root fault condition or failure occurs at the network element, this feature would have been predictable based on Hsing's teachings concerning "link or node failures." EX1003, ¶107. It would have been obvious to implement Okada-Rajala in accordance with Hsing's suggestion for restoring connections that traverse a failed node by applying Okada's restoration method to bypass an unusable link that arises from the node failure (e.g., due to a port failure at the node on a particular link). EX1003, ¶108. A POSITA would have been prompted to combine Okada-Rajala's and Hsing's teachings in this manner to improve the system's ability to handle not just fault conditions or failures originating from a problem in the link, but also those originating from a node (e.g., ATM switch). EX1003, ¶109. Connections would thus be restored more quickly for a wider range of root failures. *Id.*

Element [1.3]

Supra, Claim [6] (Section VII.A.3); EX1003, ¶110.

Claim [2]

As discussed above, it would have been obvious in view of Hsing to apply Okada's restoration process additionally when the root fault condition or failure occurs at the SENDER node ("network element"). *Supra*, Element [1.2]; EX1003, ¶¶111-114. In the resulting combination of Okada in view of Rajala and Hsing, similar priority indicators would have been applied in calculating the restoration

priority to those discussed above (Section VII.A (Claim [2])) when the root fault occurs at the SENDER node itself. *Supra*, Section VII.A (Claim [2]); EX1003, ¶113. In this circumstance, however, Okada's "capacity" and "importance" parameters would predictably relate directly to the SENDER node. *Id.* For example, Hsing discloses ATM switches (nodes) that have a "capacity" themselves apart from the link capacity. Ex-1009, 9:25-26, 9:32-34, 9:38-47, 10:13-57. In view of these teachings, it would have been obvious for Okada's "capacity" and "importance" parameters each to indicate a "severity" of the node failure and/or a "criticality" of the node, or for the "capacity" to indicate a "performance" of the node, for similar reasons to those discussed above in Section VII.A (Claim [2]); *see also* Ex-1009, 3:11-19, 3:58-4:11.

Alternatively, the additional features of claim 2 are also provided by the combined teachings of Okada and Rajala, as previously discussed. Ex-1006, [0006]; *supra*, Section VII.A (Claim [2]).

Claim [5]

Hsing discloses that "different individual users and/or different types of applications" in ATM networks often require "differing degrees of protection from service interruption." EX1009, 3:58-67; *see also id.*, 3:11-30, 3:63-67 ("assign the priority for protection on a per connection basis and offer premium services for customers requiring or desiring a high degree of protection"). The "importance"

("criticality") of a node in Hsing's system is therefore a function of its "role" or "location" in serving connections that that provide either higher or lower degrees of protection from service interruption. EX1003, ¶¶115-116; *supra*, Element [2]; EX1009, 11:54-58 ("recovery operations … vary depending on … the position of the switch 200 relative to the node or link failure"). A POSITA would have been prompted to implement the Okada-Rajala-Hsing system in accordance with Hsing's suggestion so that the criticality of the SENDER node ("network element") is determined in dependence on the location or role of the network element in the network. *Id.* Nodes serving higher-priority connections/customers would thus be prioritized over others. *Id.*

Element [8.P]

To the extent the preamble is a limitation, Okada and Rajala disclose the recited system. EX1003, ¶117. For example, Okada discloses nodes in a communication network system, and Rajala discloses a centralized NMS in communication with nodes (network elements) in a communication network system. EX1008, [0013]-[0015], FIG. 2; EX1006, [0001]-[0006], FIG. 1; *supra*, Section VII.A.3 (Element [1.3]); EX1003, ¶117.

Element [8.1.i]

Okada purports to include improve upon techniques in an ATM network, and suggests that the nodes in the communication system include switches in an ATM

network. EX1008, [0005] (citing EX1015); EX1003, ¶¶118-122. Hsing discloses additional detail about ATM switches, including that the switch can include a CPU "under control of various routines stored in [a] memory." EX1009, 8:23-24, FIG. 2; *generally id.*, 8:6-10:61 (describing various features and routines of ATM switch 200). A POSITA would have recognized that Hsing's paradigm of a CPU executing routines stored in memory corresponds to a software-based approach to handling operations at the ATM switch. EX1003, ¶¶119-120.

It would have been obvious in view of Hsing to employ a similar CPU/memory architecture in Okada's nodes to carry out various logical routines, and a POSITA would have been motivated to do so to achieve predictable benefits including increasing flexibility to program and re-program/update software routines. EX1003, ¶120. Additionally, such architectures with software-based programs were well understood and did not require specialized hardware. *Id.* The software and processing blocks of the Okada-Hsing SENDER node configured to perform the actions recited in Elements [8.1.ii]-[8.1.iii] would have provided the recited "determination unit." EX1003, ¶120.

Notably, the '211 patent does not require any particular logical or physical relationship among the functionalities that comprise processing blocks such as the determination unit (and never requires that the "unit" be implemented in a single circuit/component). EX1001, 6:60-64; EX1003, ¶¶121-122.

Element [8.1.ii]

The teachings of Okada, Rajala, and Hsing would have provided this claim element for the reasons described above in Element [8.1.i] (determination unit) and in Section VII.A.3 (Elements [1.1]-[1.2] (the first "determine" operation)). EX1003, ¶123.

Element [8.1.iii]

The teachings of Okada, Rajala, and Hsing would have provided this claim element for the reasons described above in Element [8.1.i] and in Section VII.A.3 (Element [1.3] (the second "determine" operation)). EX1003, ¶124.

Element [8.2]

Okada discloses that the priority evaluating node is configured to prioritize management actions including selection of a highest priority fault recovery message, and the selection is based on the relative priority levels reflected in recovery messages that describe the fault correction priorities for failed links in the network. EX1008, [0013] ("priority node compares the priority levels for recovery processes … to define, as the highest recovery priority fault, the fault that has the highest priority level value, and sends, to the neighboring nodes, the fault recovery message corresponding to the highest recovery priority fault and discards the other fault recovery messages"), [0014]-[0016], FIG. 1; EX1003, ¶¶125-128. As described above (Element [8.1.i]), it would have been obvious to implement logical functions

in Okada's network as software routines according to Hsing's teaching and thus the software routines configured to perform these actions in the priority node correspond to a "management activity control unit" under a first mapping of Element [8.2]. EX1003, ¶125; *cf.* EX1001, 6:60-64.

Alternatively, for the reasons previously described in the analysis of Element [1.3] (Section VII.A.3), it would have been obvious to configure Okada's SENDER node to send an alarm message containing the calculated priority level of the failed link to a centralized NMS. EX1003, ¶126. According to the teachings of Rajala, the centralized NMS prioritizes management actions such as alarm presentations and repairs/corrections of fault conditions or failures in the network. EX1006, [0006], [0013]-[0014]. Further, as discussed in Element [1.3] (Section VII.A.3), it would have been predictable for the NMS to prioritize these management actions based at least on the priority levels of received alarms. EX1003, ¶127. Likewise, for the reasons discussed above (Element [8.1.i]), a POSITA would have found it obvious and advantageous in view of Hsing to implement the centralized NMS with software routines (e.g., a "management activity control unit") programmed to carry out these functions. EX1009, 8:23-24, FIG. 2; *generally id.*, 8:6-10:61; EX1006, [0025]-[0029] & FIG. 1 (Rajala confirming that the NMS can be implemented with PC applications, servers, and other conventional computing devices); EX1003, ¶128.

Claim [9]

Supra, Claim [2]; EX1003, ¶129.

Claim [12]

Supra, Claim [5]; EX1003, ¶130.

Claim [13]

Supra, Claim [6] (Section VII.A.3); EX1003, ¶131.

Claim [14]

Supra, Claim [7] (Section VII.A.3); EX1003, ¶132.

Element [15.P]

To the extent the preamble is a limitation, Okada and Rajala disclose a network element (e.g., a SENDER node) of a communication network management system. EX1008, [Claim 1], [0013]-[0016], FIG. 1; EX1006, [0001]-[0006]; *supra*, Elements [1.2]-[1.3]; EX1003, ¶133.

Element [15.1]

The teachings of Okada, Rajala, and Hsing provide a "determination unit" configured to determine a fault correction priority in the manner recited in this claim element for at least the reasons described above in Elements [8.1.i] and [1.1]-[1.2] (Section VII.A.3 (the first "determine" operation)). EX1003, ¶134.

Element [15.2]

As discussed above, the SENDER node in a system resulting from the predictable combination of Okada, Rajala, and Hsing adds information about a

determined fault correction priority to an announcement notification. *Supra*, Elements [8.1.ii], [1.3] (Section VII.A.3 (the second "determine" operation)). For example, in a first mapping, Okada discloses that the calculated priority level (fault correction priority) is added to a fault restoration message (announcement notification) sent to management functions at neighboring/nearby nodes. EX1008, [Claim 1], [0013]-[0017], FIG. 1; EX1003, ¶136; *see also id.*, ¶¶135-139. In a second mapping based on the teachings of Okada in view of Rajala, the SENDER node would predictably add the priority level to an alarm (announcement notification) sent to a centralized NMS. *Supra*, Element [1.3] (Section VII.A.3); EX1003, ¶136. Finally, for the reasons discussed above (Element [8.1.i]), a POSITA would have found it obvious and advantageous in view of Hsing to program the network nodes with software routines configured to perform the disclosed operations. EX1009, 8:23-24, FIG. 2; *generally id.*, 8:6-10:61; EX1003, ¶138. The CPU-based software routines in the SENDER node configured to add information about the determined priority of the failed link to the announcement notifications (e.g., the alarm report or fault restoration message) provide a "message generation unit" as recited in Element [15.2]. EX1003, ¶139; *cf.* EX1001, 6:60-64.

Element [15.3]

The above-mentioned "determination unit" (refer to Elements [15.1] and [8.1.i]) in the SENDER node of Okala-Rajala-Hsing system further determines to

transmit an announcement notification to a network management function for at least the reasons described above in Element [1.3] (Section VII.A.3). EX1003, ¶140.

Claim [16]

Supra, Claim [2]; EX1003, ¶141.

Claim [19]

Supra, Claim [5]; EX1003, ¶142.

Claim [20]

Supra, Claim [6] (Section VII.A.3); EX1003, ¶143.

Claim [21]

Supra, Claim [7] (Section VII.A.3); EX1003, ¶144.

Claim [22]

Okada-Rajala and Okada-Rajala-Hsing each render obvious the method of claim 1. *Supra*, Elements [1.P]-[1.3] (Sections VII.A.3, VII.B.2); EX1003, ¶¶145-147. Further, Hsing discloses additional detail about ATM switches like Okada's network nodes, including that the switch can include a CPU "under control of various routines stored in [a] memory." EX1009, 8:23-24, FIG. 2; *generally id.*, 8:6-10:61 (describing various features and routines of ATM switch 200). For the reasons articulated above (Element [8.1.i]), it would have been obvious to implement Okada's network nodes according to Hsing's suggestion for a CPU/software framework, and in the resulting system, the SENDER node would predictably

include a memory (non-transitory computer readable storage medium) comprising computer program code, where the memory and code are configured to, with a CPU (one or more processors), cause a SENDER node (apparatus) to perform the method of claim 1. EX1003, ¶¶145-147.

C. GROUND 1C: OKADA IN VIEW OF RAJALA, HSING, AND X.733 (Claims 2, 4, 9, 11, 16, 18)

1. Overview of X.733

X.733 (EX1005) is an international standard for fault management in network systems. EX1003, ¶¶65-66. X.733 was published by the International Telecommunication Union in 1992, and was ubiquitously known by skilled artisans before the relatively late filing date of the ’211 patent (April 19, 2007). Indeed, the specification of the ’211 patent repeatedly refers to the X.733 standard and admits that the framework of the patent’s techniques is based on X.733. EX1001, 1:21-30, 3:54-56 (“the announcement notification may be an alarm notification, e.g., as specified in ITU-T X.733”), 4:13-14.

The evidence here overwhelmingly demonstrates that X.733 was publicly accessible to persons interested in communication networks before April 19, 2007. Indeed, in addition to being discussed in the background of the ’211 patent itself, many other patent publications similarly identified/discussed X.733 before the Critical Date. *See* EX1014, ¶¶9-16, Appendices E-O. Multiple patent publications

even cited and submitted copies of X.733 to the Patent Office for consideration by examiners. *See* EX1014, ¶¶9-12, Appendices E-K. X.733 was also widely discussed/cited in other technical publications before the Critical Date. *See* EX1014, ¶¶17-20, Appendices P-W. X.733 bears a copyright date of 1992, and other similar date markings, and the ITU website shows that X.733 was posted online "1992-10-26." EX1014, ¶¶5-8, Appendices A-D; *generally id.*, ¶¶1-22, Appendices A-X. Mr. Jacob Munford, an expert librarian, considered all of this evidence and assessed that X.733 was published in 1992, and certainly years before the Critical Date (April 19, 2007). EX1014, ¶¶6, 21.

2. Analysis of Okada in view of Rajala, Hsing, and X.733

Claim [2]

To the extent Okada, Rajala, and Hsing do not expressly disclose that the priority indicators for calculating a fault restoration priority includes a "perceived severity" of the detected fault condition or failure, this feature was well known as confirmed by X.733. EX1003, ¶¶148-150. X.733 describes a predetermined, standard approach for classifying faults according to "perceived severity." EX1005, 14 ("critical," "major," "minor," "warning").

X.733's suggestion for classifying faults according to their perceived severity would have been obvious to apply to Okada-Rajala-Hsing so that the SENDER node ("network element") would predictably determine the fault restoration priority of a

failed link or node based on the perceived severity of the failure. EX1003, ¶149. A POSITA would have been prompted to modify Okada-Rajala-Hsing according to X.733 in this manner to achieve predictable benefits, including use of "standardized" parameters and increasing reliability of the calculated priority level since the priority further accounts for the severity of the failure (e.g., including whether the failure impacts a "service affecting condition"). EX1003, ¶150.

Claim [4]

The Okada-Rajala-Hsing-X.733 system achieves the method of claim 2, and regarding claim 4, X.733 also details a predetermined standard for determining the perceived severity of a fault condition. EX1005, 14 ("defines six severity levels" including "cleared," "indeterminate," "critical," "major," "minor," and "warning"); EX1003, ¶151.

Claim [9]

Supra, Claim [2]; EX1003, ¶152.

Claim [11]

Supra, Claims [2], [4]; EX1003, ¶153.

Claim [16]

Supra, Claim [2]; EX1003, ¶154.

Claim [18]

Supra, Claims [2], [4]; EX1003, ¶155.

D. GROUND 1D: OKADA IN VIEW OF RAJALA, HSING, X.733, AYANOGLU, AND PARSA (Claims 2-3, 9-10, 16-17)

1. Analysis of Okada in view of Rajala, Hsing, X.733, Ayanoglu, and Parsa

Claim [2]

X.733 discloses alarm parameters that define predetermined environmental conditions including "flood detected" (e.g., water level), "humidity unacceptable," and "temperature unacceptable." EX1005, 11-13. It would have been obvious to a POSITA to relate the priority of a link failure at a SENDER node in an ATM network as taught by Okada and Hsing to a temperature condition, as demonstrated by Ayanoglu and Parsa. EX1003, ¶¶156-160.

For example, Ayanoglu teaches that ATM networks can be implemented as an ad-hoc network of wireless access points. EX1010, 1:16-19 ("The present invention relates to packet-based telecommunications networks, and more particularly to a restoration mechanism for use in ATM networks having wireless links."), 2:16-17 ("ATM cells are transported over a wireless point-to-point link"), 1:58-64; EX1003, ¶67.

Parsa further discloses known techniques for wireless access points that include "temperature control functionality that is adapted to control/moderate the temperature within an access point." EX1011, Abstract; EX1003, ¶68. Parsa explains that "[i]ncreasing temperatures may translate to increased noise, reduced

system reliability, e.g., reduced mean time between failure (MTBF), and potential failure of one or more system components," and "[p]erformance attributes of system components may be altered and/or negatively impacted by heat conditions, thereby reducing system performance from optimal levels." Parsa proposes to mitigate potential damage resulting from temperature overages by "reducing access point throughput" and/or "reducing transmission power" from the access point while the temperature is exceeds safe operating limits. *Id.*, [0022], [0050], [0054], [0063]-[0065], FIG. 9.

A POSITA would have found it obvious to apply the teachings of Ayanoglu and Parsa in combination with Okada-Rajala-Hsing such that the ATM network in the resulting system includes wireless nodes/switches. EX1003, ¶¶159-160. For example, wireless nodes/switches would have been beneficial to apply in Okada when transmission lines and wired infrastructure is either unavailable or too expensive to implement to connect two or more nodes in the network. *Id.* Further, a POSITA would have recognized that link failures can occur due to high-temperature conditions. EX1003, ¶160. It would have been obvious to account for the temperature of the node/switch (e.g., how much the temperature exceeds a safe operating limit) based on Parsa's teaching when computing the "relative priority level" of a failed link since the temperature overage would inform the severity of the failure and/or the amount of time before the node/switch returns to a safe operating

level. EX1003, ¶ 160(citing EX1015 and EX1018 to corroborate analysis).

Claim [3]

For the same reasons already detail above (analysis of Claim [2]), the resulting combination would likewise provide the predetermined environmental condition of claim 3. EX1003, ¶161.

Claim [9]

Supra, Claim [2]; EX1003, ¶162.

Claim [10]

Supra, Claims [2], [3]; EX1003, ¶163.

Claim [16]

Supra, Claim [2]; EX1003, ¶164.

Claim [17]

Supra, Claims [2], [3]; EX1003, ¶165.

E. GROUND 2A: NAKAMURA IN VIEW OF X.733 AND RAJALA (Claims 1-21)

1. Overview of Nakamura

Nakamura describes "a network system having a plurality of network elements and a monitoring device for monitoring the network elements." EX1004, 1:9-11; *see also id.*, 1:12-54, 2:41-3:14, FIG. 1 ("conventional" system) & 3:15-4:30, FIG. 2 ("preferred embodiment"); EX1003, ¶¶69-73. Similar to the '211 patent, Nakamura recognized that the "conventional" approach of network elements

reporting many fault signals to a centralized monitoring device renders effective monitoring or supervising functions especially difficult due to the high volume of fault signals. *Id.*, 1:49-54, 3:14 (same). Nakamura also addressed this problem in a like manner to the '211 patent—albeit years earlier. *Id.*, 3:15-4:3, FIG. 2; *see also id.*, 1:58-2:30.

Figure 2 shows Nakamura's purportedly improved network element, which includes a "classifying circuit 23" to assess the classification or rank of each fault, along with a "selecting circuit 25" to select the compact rank signals or detailed fault signals for transmission:

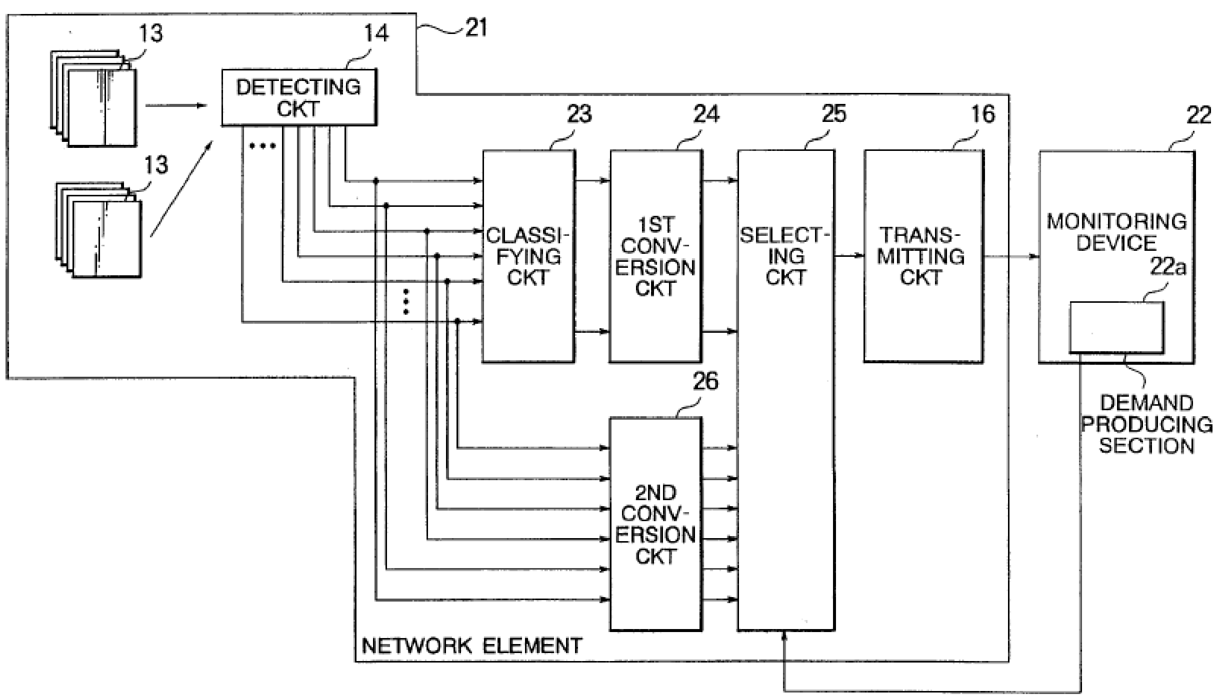


FIG. 2

EX1004, FIG. 2.

2. Analysis of Nakamura in view of X.733 and Rajala

Element [1.P]

To the extent the preamble is a limitation, Nakamura discloses the recited method. EX1004, 3:15-4:30 & FIG. 2 (describing a method of processing fault signals with circuitry in a network element); *see also id.*, [0009] ("method"), claim 30; EX1003, ¶166.

Element [1.1]

The teachings of Nakamura in view of X.733 and Rajala provide this claim element. EX1003, ¶¶167-179. For example, Nakamura's network element 21 includes a collection of network units 13 configured to "carry out a network process in cooperation with one another." EX1004, 2:51-52, FIG. 2. When first through N-th faults occur in the network units, detecting circuit 14 detects the faults and "produce[s] first through N-th fault signals, respectively." *Id.*, 2:57-59; *see also supra*, Section VII.E.2. "The first through N-th fault signals are representative of detail messages of the first through the N-th faults, respectively." EX1004, 2:59-62; *see also id.* 3:15-26 (describing similarities between portions of the systems depicted in FIG. 1 and FIG. 2), 1:21-22. The fault signals are provided to classifying circuit 23, which classifies the fault signals and "judges whether or not the fault degree of each of the … fault signals" falls within one of M predetermined fault levels (where 1<M<N). *Id.*, 3:24-43.

To the extent Nakamura does not expressly disclose the detailed contents of the first through N-th fault signals, X.733 describes a range of well-known parameters that were commonly included in network-based fault announcements. EX1005; EX1003, ¶¶168-169; *supra*, Section VII.E.2; *cf.* EX1001, 1:21-27, 3:54-56, 4:13-14 (admissions in the '211 patent concerning the applicability of X.733 to fault reporting). Specifically, X.733 provides that an announcement notification (e.g., alarm) for a fault event should include an "**event type**" parameter that indicates a classification of the alarm into one of "[f]ive basic categories": "communications alarm type," "quality of service alarm type," "processing error alarm type," "equipment alarm type," or "environmental alarm type." *Id.*, 11. X.733 further prescribes standards for reporting "**specific information**" about a fault event. *Id.* Among others, the "specific information" disclosed in X.733 includes information about "probable cause," "specific problems," "perceived severity," "backed-up status," "back-up object," "trend indication," "threshold information," and "proposed repair actions." *Id.*, 12-16.

A POSITA would have found it obvious to implement Nakamura in accordance with X.733's standardized parameters for fault reporting such that Nakamura's first through N-th fault signals would each include "event type" and "specific information" parameters like those disclosed in X.733. EX1003, ¶170. Multiple reasons would have motivated a POSITA to modify Nakamura in view of

X.733 in this manner. *Id.*

First, X.733's "event type" and "specific information" parameters would have improved Nakamura's system by providing details about fault events in network units 13 that would enhance the ability of the classifying circuit 23 to classify/rank fault signals, and that would further enhance the central monitoring device's 22 ability to monitor/supervise faults across a network (e.g., upon the monitoring device's demand for fault signals from particular network elements). EX1003, ¶171. X.733 explains that "[e]arly detection of faults before significant effects have been felt by the user is a desirable requirement of communicating systems," and the X.733 reporting parameters provide key information to inform the nature and priority of faults in network elements. EX1005, 10; *id.*, 7 ("The alarm notifications defined by this function provides information that a manager may need to act upon pertaining to a system's operational condition and quality of service."). For example, a POSITA would have recognized that the event type, perceived severity, backed-up status, severity trend indication, and threshold parameters all bear on the "significance" (and thus "priority") of a fault—which is precisely what Nakamura seeks to evaluate with the classifying circuit 23. EX1004, 3:28-42; *see also id.*, EX1005, 15 ("managing system [] monitors the Perceived severity parameter in received alarm reports"). The evidence here confirms it was known that "[t]he importance of the alarms mainly depends on two factors: 1) the effect of

the alarm on the performance of the network element, and 2) the importance of the network element." EX1006, [0006]; EX1003, ¶171. Accordingly, applying X.733's fault parameters to Nakmura's fault signals to facilitate classification and monitoring of faults in network elements would have been entirely predictable by the late filing date of the '211 patent (April 19, 2007). EX1003, ¶171.

Second, a POSITA would have been prompted to implement Nakamura's fault signals in accordance with the teachings of X.733 since X.733 was a well-known, international standard for fault management in the relevant timeframe (e.g., April 19, 2007). EX1003, ¶172. X.733 emphasized the importance of "provid[ing] alarm reports with a standardized style, using a common set of notification types." EX1005, 10. This would allow a managing system such as the monitoring device that receives fault signals from a range of different network elements and network units across a network to process the fault signals in a standardized format, regardless of the type of network element or unit from which the signal originated. EX1003, ¶172.

Third, a POSITA would have recognized that the architecture of Nakamura's system falls squarely within the types of systems for which X.733 was developed. X.733 was intended to be widely applicable for fault reporting by any "managed object" in a network. EX1005, 10 ("The notification types specified in this function are intended to be generally applicable and can be imported into the definition of

any managed object."). The background discussion of the '211 patent admits that the concept of "managed objects" was well-known, and acknowledges that network elements could each encompass a collection of "managed objects" that were each capable of detecting/reporting fault conditions. EX1001, 1:14-20 ("[T]he network elements comprise a plurality of physical and logical devices/resources/functions. These are called 'managed objects' in the context of network management."). Consistent with the framework outlined in X.733 (and corroborated by the '211 patent background), Nakamura's network elements each include a collection of network units 13 for which the system generates fault signals. The network units 13 are akin to "managed objects" in the X.733 framework, and it would have been predictable for X.733 to apply in this highly similar context. EX1003, ¶173.

Nakamura also teaches that fault signals are processed by the classifying circuit 23 to generate classified signals indicative of the degree or significance of a fault, and the fault signals can be sent on demand in a message signal sequence to the monitoring device 22 to permit "exact" monitoring of a network element. EX1004, 3:15-58, 4:4-30, FIG. 2. Nonetheless, to the extent Nakamura does not expressly disclose use of the fault signals "for a fault correction" as recited in claim 1, this feature would have been obvious based on Rajala's teachings. EX1003, ¶174; *supra*, Section VII.A.2. Rajala discloses that network fault management is traditionally "based on monitoring alarms, evaluating their importance and effects,

and accordingly, on initiating repairs." EX1006, [0006]; *generally id.*, [0001]-[0013]; *cf.* EX1001, 1:65-2:4, FIG. 6. A POSITA would have found it predictable to further modify Nakamura-X.733 in view of Rajala such that the central monitoring device 22 further processes the signals received from a network element to inform decisions on fault corrections. EX1003, ¶174. In this context, the fault signals in the resulting system would predictably include content "defining at least two priority indicators for a fault correction," as recited in claim 1. *Id.* For example, as discussed, a straightforward implementation of Nakamura's system in accordance with X.733 would involve parameterizing the fault signals with the alarm parameters disclosed in X.733. EX1003, ¶174.

The parameters of X.733's alarm indicate a priority for a fault correction in at least two ways. First, as discussed below with respect to Element [1.2], it would have been obvious for Nakamura's classifying circuit 23 to process at least two of the X.733 alarm parameters in the fault signals to determine classifications or ranks of the fault signals. *Infra*, Element [1.2]; EX1003, ¶175. The classification/rank of the fault signals are reported to the monitoring device 22, which then determines based on the rank signal sequence whether further monitoring of the network element is necessary. EX1004, 3:65-4:13. The monitoring device 22 thus prioritizes monitoring (and fault correction actions according to Rajala) of different network elements based on the rank signal sequence that would be derived from the X.733

alarm parameters in the fault signals in the Nakamura-X.733-Rajala system. EX1003, ¶175. Second, the X.733 alarm parameters in the fault signals serve to indicate a priority for a fault correction when the alarm parameters are transmitted on demand in the "message signal sequence" to the monitoring device 22. EX1004, 4:14-30, EX1003, ¶175. Indeed, the "message signal sequence" is merely a protocol-converted version of the fault signals themselves, and therefore the message signal sequence would predictably include the detailed contents (including the X.733 parameters) of the fault signals themselves. EX1004, 3:59-64, FIG. 2; EX1003, ¶175. As taught by Rajala and suggested by X.733, it was well-known for a monitoring device in a centralized network management system to prioritize fault repairs/corrections based on parameters in the signals that indicate "the effect of the alarm on the performance of the network element" and "the importance of the network element." EX1006, [0006]. A POSITA would have recognized that the ordinary X.733 parameters (e.g., perceived severity, trend indication, threshold information, event type, backed-up status, probable cause) bear on factors such as these that conventionally inform fault correction priorities. EX1003, ¶176.

Multiple reasons would have prompted a POSITA to further modify Nakamura-X.733 in view of Rajala's suggestion for prioritizing fault corrections. EX1003, ¶¶176-177.

First, by using the X.733 parameters to inform fault correction actions, the

system would predictably benefit from faults actually being corrected (rather than merely "monitored"). EX1003, ¶177.

Second, a POSITA would have recognized that, by using the X.733 parameters to prioritize fault corrections, the system would predictably benefit by allowing limited repair resources to be directed to more significant faults before less significant faults. EX1006, [0006] ("focus the repairs efficiently"); EX1003, ¶¶178-179.

Element [1.2]

The teachings of Nakamura in view of X.733 and Rajala provide this claim element. EX1003, ¶¶180-185. As discussed above (Element [1.1]), it would have been obvious to implement Nakamura in accordance with X.733 and Rajala such that Nakamura's fault signals would include standard alarm parameters like those disclosed in X.733 and the monitoring device 22 would predictably prioritize fault corrections as suggested by Rajala. *Supra*, Element [1.1]; EX1003, ¶¶180. The system based on Nakamura, X.733, and Rajala would determine at a network element (e.g., Nakamura's network element 21) of a communication network management system (e.g., Nakamura's network communication system including management functions like those disclosed in X.733 and Rajala) classified signals for a set of fault signals 1-N that indicate a significance (e.g., fault sublevel or ranking) of the fault signals according to the ordinary function of Nakamura's

classifying circuit 23. EX1004, 3:28-31 ("the predetermined fault level is classified into first through M-th fault sublevels or ranks each of which defines a fault degree representative of significance of the fault"), 3:39-42, 3:49-51, FIG. 2. The classifying circuit 23 determines the classified signals (alarms) in response to a detection of a fault condition or failure at the network element, such as in response to a detection of faults in the network units 13. EX1004, 2:53-54 ("first through N-th faults may occur in the network units"), 2:56-59, 3:22-28. For instance, Figure 2 of Nakamura shows that the classifying circuit 23 generates the classified signals in response to receiving the fault signals from detecting circuit 14. *Id.*, FIG. 2.

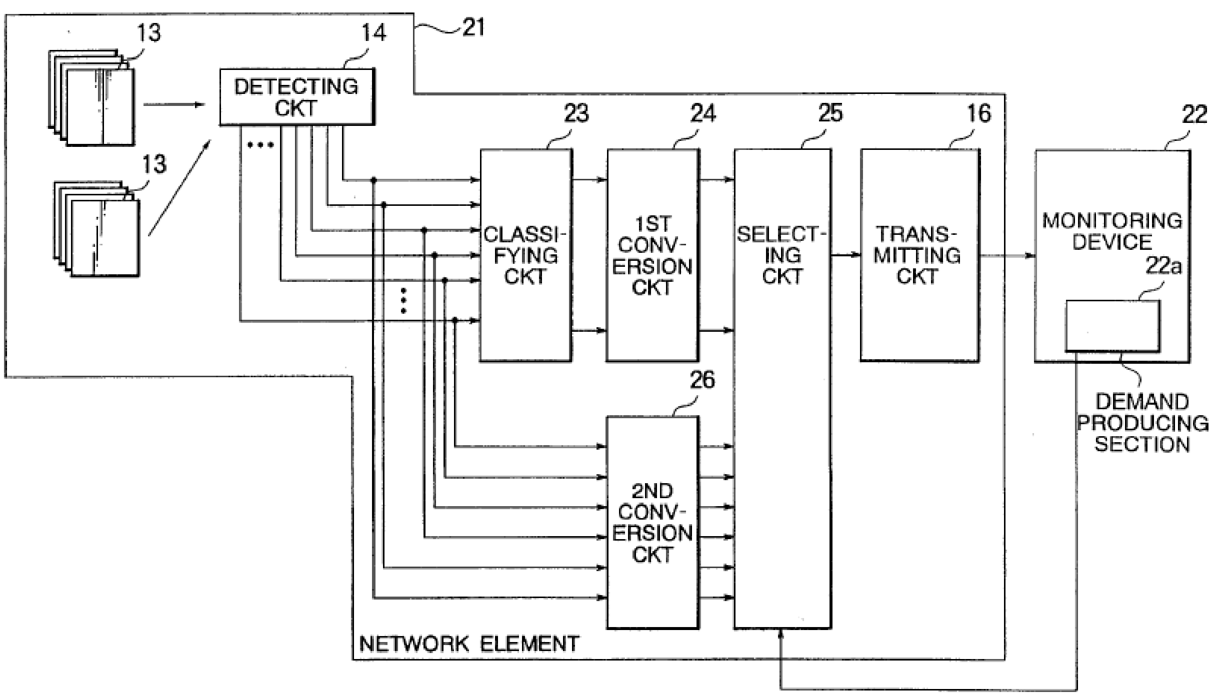


FIG. 2

EX1004, FIG. 2.

The classified signal(s) (and/or representations of the classified signals such as the protocol-converted rank signals or rank signal sequence) correspond to a "fault correction priority" as recited in claim 1. EX1003, ¶181. It would have been obvious according to Nakamura and X.733 for the classifying circuit 23 to determine the classified signals based on at least two X.733 standard alarm parameters (at least two priority indicators) that are embedded in the one or more fault signals. EX1003, ¶182; *cf.* EX1001, 5:36-38 ("The priority attribute/parameter can be … a bit string, a number, a character, a word, or any combination and plurality of those.").

Based on Nakamura, it would have been obvious for the classifying circuit 23 to classify each individual fault signal into a particular fault sublevel based on at least two of the X.733 alarm parameters from that fault signal. EX1003, ¶182. This follows from Nakamura's suggestion that the classified signals represent an overall degree/significance of a fault derived from the more detailed fault message signals, and the evident relevance of various X.733 parameters to the overall degree/significance of a fault. EX1004, 2:59-62, 3:28-53.

For instance, the "perceived severity" parameter from X.733 indicates the degree to which a fault has affected a service condition of the network unit, the "backed-up status" parameter indicates whether services from the network unit have been backed-up to prevent service disruption, the "trend indication" parameter indicates changes in the perceived severity, and the "threshold information"

parameter indicates by how much a measured value exceeded a threshold triggering an alarm or fault condition. EX1005, 10-15. A POSITA would have recognized that all of these parameters inform the degree/significance of a fault (and thus the priority of a fault correction), and as such, it would have been predictable to classify a fault signal based on all or some of these parameters as disclosed in X.733. EX1003, ¶183. By way of example, a fault with a higher perceived severity for a network unit with service that is not backed-up may be more significant and require higher priority correction than a fault with a same or lower severity level for a network unit with service that has been backed up since there is a greater likelihood of service disruption arising from the former fault. *Id.*, ¶183; *see also* EX1005, 14 ("use of [the backed-up status] field in conjunction with the severity field provides information in an independent form to quality the seriousness of the alarm"); EX1006, [0006] ("The importance of the alarms mainly depends on two factors: 1) the effect of the alarm on the performance of the network element, and 2) the importance of the network element."). This would have been predictable considering the similar function of the classifying circuit 23 in ranking/classifying faults as ordinary network management devices, which conventionally prioritized faults based on multiple priority indicators. EX1003, ¶183.

Moreover, Nakamura suggests that each of the classified signals is based on an accumulation of the classifications of the fault signals belonging to a particular

fault sublevel. EX1004, 3:43-53 (describing "first and second classified signals which [are] called major and minor alarms, respectively," where each classified signal is based on the fault signals that all fall within a corresponding fault sublevel). As a result of this accumulation, the classified signals are further based on information (e.g., X.733 parameters) spanning multiple fault signals when more than one fault signal is classified within a particular fault sublevel. Therefore, the "at least two priority indicators" can additionally or alternatively be provided in different fault signals that are classified within the same fault sublevel. EX1003, ¶184. The classified signals (and/or representations of the classified signals such as rank signals or a rank signal sequence) are utilized for fault correction priority for the reasons discussed above. *Supra*, Element [1.1]; EX1003, ¶¶184-185.

Element [1.3]

As described above (Element [1.1]-[1.2]), it would have been predictable to apply teachings from X.733 and Rajala to Nakamura's system such that the classifying circuit 23 at network element 21 determines a fault correction priority (e.g., classified signal/rank signal/rank signal sequence) based on at least two priority indicators for a fault correction (e.g., X.733-like alarm parameters from one or more fault signals). EX1003, ¶186; *supra*, Elements [1.1]-[1.2]. Nakamura further discloses that the network element determines to transmit (and does transmit) a "first monitoring signal" (e.g., an "announcement notification") to a monitoring

device 22 (e.g., a "network management function"). EX1004, 3:52-57, 3:65-4:3, FIG. 2. The first monitoring signal indicates a fault condition or failure, especially since Nakamura expressly discloses that the "first monitoring signal" corresponds to the "rank signal sequence," and the "rank signal sequence" in turn represents alarms (e.g., major and minor alarms) indicative of fault conditions or failures that occurred at one or more network units 13 in the network element 21. EX1004, 2:50-56, 3:48-4:3, FIG. 2. The formulation of a "first monitoring signal" or "rank signal sequence" by its very nature indicates a fault condition or failure at a network element since the purpose of the first monitoring signal is to report information indicative of fault conditions (and a POSITA would have expected that no such signals would be generated in the absence of a fault condition or failure). EX1003, ¶186. The "first monitoring signal" (e.g., "announcement notification") also specifically includes information about the determined fault correction priority (e.g., classified signal/rank signal/rank signal sequence) since Nakamura explains that "[t]he transmitting circuit 16 transmits the rank signal sequence as a first monitoring signal." EX1004, 4:1-3. The determination to transmit the "rank signal sequence" in the "first monitoring signal" is made by circuitry including the "selecting circuit 25" based on receipt of a new rank signal sequence from the "first conversion circuit 24." *Id.*, 3:53-4:1, FIG. 2.

Claim [2]

As discussed above (Elements [1.1]-[1.2]), it would have been obvious to modify Nakamura in view of X.733 such that Nakamura's detailed fault signals incorporate the standard alarm parameters described in X.733 ("at least two priority indicators"). *Supra*, Elements [1.1]-[1.2]; EX1003, ¶¶187-189. Among the alarm parameters described in X.733 that would have been obvious to apply in Nakamura are those relating to event type, probable cause, specific problems, perceived severity, back-up status, back-up object, trend indication, proposed repair actions, and/or threshold information. *Id.*; EX1005, 10-16. The "perceived severity" parameter indicates a "perceived severity" of a detected fault condition or failure, as recited in claim 2. EX1005, 14. The "back-up status" parameter indicates a "criticality" of the network element since it indicates whether a service has been backed-up such that service interruption is avoided. *Id.* ("use of this field in conjunction with the severity field provides information in an independent form to qualify the seriousness of the alarm and the ability of the system as a whole to continue to provide services"). The "threshold information" parameter indicates a performance of the network element since it provides an "observed value" of a "gauge or counter" measuring an aspect of the network element's performance. *Id.*, 15; EX1003, ¶188. Certain values of the "probable cause" parameter indicate at least one predetermined environmental condition, such as "excessive vibration,"

"fire detected," "flood detected," "humidity unacceptable," "temperature unacceptable," or "toxic leak detected." EX1005, 11-13. Other values of the "probable cause" parameter also indicate a performance of the network element, such as "bandwidth reduced," "congestion," "corrupt data," "CPU cycles limit exceeded," "degraded signal," "equipment malfunction," "out of memory," or "resource at or nearing capacity." *Id.*

Claim [3]

As discussed above (Elements [1.1]-[1.2]), X.733 discloses alarm parameters that would have been obvious to utilize as priority indicators for classifying fault signals in Nakamura's system. EX1003, ¶190. The X.733 alarm parameters define predetermined environmental conditions including "flood detected" (e.g., water level), "humidity unacceptable," and "temperature unacceptable." EX1005, 11-13. For example, a flood indicator may reflect a fault requiring higher priority correction than a humidity indicator since the humidity will ordinarily recede with external environmental conditions while a flood is more likely to present immediate and long-lasting problems such as electrical shorts and corrosion if corrective action is not taken. EX1003, ¶190; *supra*, Element [2].

Claim [4]

X.733 describes a predetermined standard for determining the perceived severity of a fault condition. EX1005, 14 ("defines six severity levels" including

"cleared," "indeterminate," "critical," "major," "minor," and "warning"); EX1003, ¶191.

Claim [5]

As discussed above (Elements [1.1]-[1.2]), X.733 discloses alarm parameters that would have been obvious to utilize as priority indicators for classifying fault signals in Nakamura's system. EX1003, ¶¶192-193. The X.733 alarm parameters define a "back-up status" parameter that indicates a "criticality" of a network element since it indicates whether a service has been backed-up such that service interruption is avoided. EX1005, 14 ("use of this field in conjunction with the severity field provides information in an independent form to qualify the seriousness of the alarm and the ability of the system as a whole to continue to provide services"). For example, X.733 explains that a managed object may be in "a pool of objects any of which may be dynamically allocated to replace a faulty object." *Id.* Thus, when a network element includes a faulty network unit (akin to a managed object) that provides a service that can be dynamically re-allocated to another network unit on the same or different network element (e.g., a "pool" of backed-up network units), the back-up status parameter (and back-up object parameter) is determined in dependence on the "role" of the network element. EX1003, ¶¶193. A network element that offers a service through a network unit that cannot be backed-up serves a more critical and unique "role" in the network than a network element that offers

the service through a network unit that can be backed up. *Id.*

Claim [6]

Rajala prioritizes repairs of network elements based on metrics that indicate how much current traffic conditions during a fault condition or failure deviate from normal traffic conditions prior to the fault condition or failure. EX1006, [0037] ("calculate a normal value, a current value and/or a relative or an absolute deviation from the normal value"), [0012]-[0013], [0038], [0043] ("amount of traffic"), [0044], FIG. 6; EX1003, ¶¶194-198. Calculating the deviation between the normal and current traffic loads involves "comparing" the traffic load prior to and during a detected fault condition since "deviation" is a measure of how much the current load has departed from the normal load. *Id.*

A POSITA would have found it obvious to further modify Nakamura in view of Rajala such that the fault signals for appropriate network units would include a parameter describing the deviation of the current traffic load after the detected fault to the normal load before the fault in accordance with Rajala's teachings here. EX1003, ¶196. Multiple reasons would have prompted a POSITA to implement such a modification. **First**, the approach is consistent with Nakamura's and X.733's suggestion that fault signals and alarm reports should include detailed information concerning detected fault conditions. EX1004, 2:59-62; EX1005, 6-10; EX1003, ¶197. X.733 similarly discloses alarm reports having detailed measurement values

in the "threshold information" parameter. EX1004, 15. **Second**, as expressly described in Rajala, measuring deviation in traffic load is important in assessing the significance/degree of a fault condition, and in prioritizing repairs, and the result would have been predictable. *Id.*, [0012]-[0013]; EX1003, ¶198.

Claim [7]

Nakamura discloses that the "first monitoring signal" (e.g., an "announcement notification") contains a rank signal sequence describing the classified signals from classifying circuit 23. EX1004, 3:53-4:3, FIG. 2. The classified signals are representative of "alarms." *Id.*, 3:48-51 ("classifying circuit 23 produces first and second classified signals which will be called major and minor alarms, respectively"). Therefore, Nakamura's announcement notification is an "alarm notification" as recited in claim 7. EX1003, ¶¶199-200; *see also id.*, EX1005, 10 (describing "alarm" reports).

Element [8.P]

To the extent the preamble is a limitation, Nakamura discloses the recited system. EX1004, 1:9-11 ("network system having a plurality of network elements and a monitoring device"), 1:58-67, 2:36-37, FIG. 2; EX1003, ¶201.

Element [8.1.i]

In Nakamura-X.733-Rajala (*see supra*, Elements [1.1]-[1.3]), circuits 14 and 23-26 cooperate to perform each of the actions recited in Elements [8.1.ii] and

[8.1.iii]. The portions/circuits of network element 21 configured to perform these recited actions from Elements [8.1.ii] and [8.1.iii] provide the recited "determination unit." EX1003, ¶¶202-204. For example, the determination unit encompasses classifying circuit 23, which is configured to determine the classified signals that represent a "fault correction priority" in the Nakamura-X.733-Rajala system. EX1004, 3:24-52; EX1003, ¶¶202-203. The determination unit further encompasses the selecting circuit 25, which selects the rank signal sequence for transmission and thus determines to transmit the rank signal sequence as a first monitoring signal ("announcement notification") to the monitoring device ("network management function"). EX1003, ¶203. Optionally, the determination unit further encompasses first conversion circuit 24, which performs protocol conversion on the classified signals to generate the rank signals and rank signal sequence (EX1004, 3:53-57), and transmitting circuit 16, which transmits the rank signal sequence as a first monitoring signal to the monitoring device 22 (EX1004, 4:1-3). EX1003, ¶¶203-204. Each of these circuits is disposed in a network element apart from the network units 13, and would be considered a "unit" as that term is used in the '211 patent. *Id.*; *cf.* EX1001, 6:60-64; EX1003, ¶204.

Element [8.1.ii]

The above-mentioned components of network element 21 (refer to Element [8.1.i]) in the Nakamura-X.733-Rajala system are configured to perform this first

"determine" operation for the same reasons described above in Elements [1.1]-[1.2]. EX1003, ¶205.

Element [8.1.iii]

The above-mentioned components of network element 21 (refer to Element [8.1.i]) in the Nakamura-X.733-Rajala system are configured to perform this second "determine" operation for the same reasons described above in Element [1.3]. EX1003, ¶206.

Element [8.2]

Nakamura discloses that "[s]upplied with the first monitoring signal, the monitoring device 22 judges whether or not it is necessary to exactly monitor the network element 21." EX1004, 4:4-12; *see also id.*, 4:14-30, FIG. 2. "The monitoring device 22 decides whether or not it is necessary to obtain the message signal sequence on the basis of the rank signal sequence." EX1004, 4:24-28. Through these operations, the monitoring device (network management function) prioritizes management actions (e.g., prioritizes "exact" monitoring of network elements) based on the information about the determined fault correction priority (e.g., based on the classification and rank signal information reflected in the first monitoring signal). EX1003, ¶¶207-209.

Further, a POSITA would have recognized that the monitoring device 22 performs a number of functions including evaluating first monitoring signals and

evaluating second monitoring signals to exercise supervision over the network elements. EX1003, ¶208. The portion of the monitoring device 22 configured to evaluate the first monitoring signal and determine whether to demand the more detailed second monitoring signal provides a "management activity control unit," as recited in claim 8. EX1003, ¶208; *cf.* EX1001, 6:60-64. As an alternative mapping, the portion of the monitoring device configured to evaluate the second monitoring signal can also correspond to the "management activity control unit," since the monitoring device 22 in the Nakamura-X.733-Rajala combination is configured to prioritize alarm presentations and repairs/corrections (e.g., management actions) based on information contained in the fault signals reflected in the second monitoring signal (and the determined fault classifications or rankings from the first monitoring signal). EX1003, ¶208; *supra*, Elements [1.1]-[1.3].

Claim [9]

Supra, Claim [2]; EX1003, ¶210.

Claim [10]

Supra, Claim [3]; EX1003, ¶211.

Claim [11]

Supra, Claim [4]; EX1003, ¶212.

Claim [12]

Supra, Claim [5]; EX1003, ¶213.

Claim [13]

Supra, Claim [6]; EX1003, ¶214.

Claim [14]

Supra, Claim [7]; EX1003, ¶215.

Element [15.P]

To the extent the preamble is a limitation, Nakamura discloses a network element of a communication network management system. EX1004, 3:15-33 ("network element 21" and "network system"), FIG. 2; *see also* EX1005, 1 ("communication networks"), 7 ("systems management function"), 9; EX1006, [0001] ("monitoring and maintaining a network in telecommunications"); EX1003, ¶216.

Element [15.1]

The above-mentioned components of network element 21 (refer to Element [8.1.i]) in the Nakamura-X.733-Rajala system provide a "determination unit" that determines a "fault correction priority" in the manner recited in this element for the same reasons described above in Elements [1.1]-[1.2]. EX1003, ¶217.

Element [15.2]

Nakamura discloses "[t]he first and the second classified signals are delivered from the classifying circuit 23 to a first conversion circuit 24 to be protocol converted into first and second rank signals," which are then "supplied as a "rank

signal sequence" from the first conversion circuit 24 to a selecting circuit 25." EX1004, 3:53-57, FIG. 2. "The selecting circuit 25 selects the rank signal sequence … to deliver the rank signal sequence as a selected signal to the transmitting circuit 16." *Id.*, 3:65-4:1. "The transmitting circuit 16 transmits the rank signal sequence as a first monitoring signal to the monitoring device 22." *Id.*, 4:1-3. The network element 21 is therefore configured to add an information about the determined fault correction priority (e.g., by adding the rank signal sequence that includes information about the classification of fault signals and major/minor alarms) to an announcement notification (e.g., first monitoring signal). EX1003, ¶218. The circuitry in the network element 21 configured to perform these actions (e.g., the first conversion circuit 24, selecting circuit 25, and/or transmitting circuit 16) provide a "message generation unit" as recited in claim 15. EX1003, ¶219; *cf.* EX1001, 6:60-64.

Element [15.3]

The above-mentioned components of network element 21 (refer to Element [8.1.i]) in the Nakamura-X.733-Rajala system are further configured to determine to transmit an announcement notification (e.g., first monitoring signal) in the manner recited in this element for the same reasons described above in Element [1.3]. EX1003, ¶220.

Claim [16]

Supra, Claim [2]; EX1003, ¶221.

Claim [17]

Supra, Claim [3]; EX1003, ¶222.

Claim [18]

Supra, Claim [4]; EX1003, ¶223.

Claim [19]

Supra, Claim [5]; EX1003, ¶224.

Claim [20]

Supra, Claim [6]; EX1003, ¶225.

Claim [21]

Supra, Claim [7]; EX1003, ¶226.

F. GROUND 2B: NAKAMURA IN VIEW OF X.733, RAJALA, AND NATARAJAN (Claim 22)

1. Analysis of Nakamura in view of X.733, Rajala, and Natarajan

Claim [22]

Nakamura in view of X.733 and Rajala renders obvious the method of claim 1. *Supra*, Elements [1.P]-[1.3] (Section VII.E.2); EX1003, ¶¶74, 227-229. Further, Natarajan discloses a known network device that employ "one or more memories … configured to store data and/or store program instructions for [] general-purpose network operations and other specific functions … ." EX1007, 6-11, FIG. 5A;

generally id., 12:6-38. Natarajan further discloses "machine readable media that include program instructions, operating information, etc. for performing various operations … ." *Id.*, 12:20-26.

It would have been obvious to further modify the network element in the system of Nakamura-X.733-Rajala in view of Natarajan such that the network element employs the predictable hardware and software-based components disclosed in Natarajan. The resulting network element would include a non-transitory computer-readable storage medium comprising computer program code, said computer-readable storage medium and said computer program code configured to, with one or more processors, cause an apparatus (e.g., network element) to at least perform the method of claim 1. EX1003, ¶228. A POSITA would have been prompted to apply Natarajan's suggestion concerning the configuration/components of a network device in the resulting combination to achieve known benefits associated with such configuration/components, including an ability to flexibly program and update capabilities of the network element simply by loading program code into memory. EX1003, ¶229. Additionally, the components described in Natarajan were ordinary and widely available, and would have been a preferred solution as of the relatively late filing date of the '211 patent (April 19, 2007). *Id.*, ¶229.

VIII. INSTITUTION SHOULD NOT BE DISCRETIONARILY DENIED

In *Apple Inc. v. Fintiv, Inc.*, the Board enumerated six factors that provide a "holistic view" as to "whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in [a] parallel proceeding." IPR2020-00019, Paper 11 at 2-3 (PTAB "precedential" Mar. 20, 2020) ("*Fintiv I*"). Guided by precedent, Huawei took affirmative steps to promote the Board's efficiency and fairness goals. Huawei initiated this proceeding with exceptional diligence, filed a single petition within a mere 9 weeks of learning of WSOU's asserted claims, and provided a stipulation akin to *Sand Revolution* to eliminate overlapping prior art grounds between the instituted IPR proceeding and the Related Litigation. EX1102. These facts, paired with the strong merits of Grounds 1-2, provide compelling reasons to institute. *Sand Revolution II, LLC v. Continental Intermodal Group*, IPR2019-01393, Paper 24, 12 (PTAB "Informative" June 16, 2020).

Relevant Facts— Between September 29, 2020 and October 2, 2020, WSOU filed six separate infringement actions against Huawei involving six unrelated patents asserted against several unrelated products. *See* EX1100. These six lawsuits are concurrently pending in the Western District of Texas ("the Court") before the Honorable Judge Alan D. Albright. *Id*. The action involving the '211 patent was assigned Case No. 6:20-cv-00893 ("the Related Litigation"). The remaining

lawsuits are identified by different cases numbers and are not formally consolidated. The district court's scheduling order indicates that they will be consolidated into two or more groups—with a trial for the "first of the consolidated cases" starting on September 26, 2022 and a subsequent trial(s) for the "remaining consolidated cases" on a later (unknown) date. EX1101, 5.

WSOU served its preliminary infringement contentions on February 5, 2021, but oddly characterized the contentions as "confidential" and did not authorize Huawei's in-house counsel to view the charts of the preliminary infringement contentions until February 24, 2021. *See* EX1101, 1. As such, this Petition was filed just nine weeks after initially learning of the asserted claims and about six weeks after actually viewing infringement charts. This Petition was served on Patent Owner even before Huawei's preliminary invalidity contentions, which are not due until April 12, 2021 (extended from April 7 upon agreement from the parties). *Id*.

The Court set a *Markman* hearing for August 12, 2021, and the parties are scheduled to exchange terms for construction on April 16, 2021. *See* EX1101, 2-3. Per the Court's default order, fact discovery will formally open on August 16, 2021, two business days after the *Markman* hearing. *See* EX1101, 3. In other words, little discovery—and certainly no meaningful expert discovery regarding invalidity of the '211 patent—will be completed at the time of the Board's institution decision here.

For purposes of planning earlier dates throughout discovery, etc., the Court

set two placeholder trial dates—a first trial starting on September 26, 2022 for an unknown "first" subset of the six asserted patents and a subsequent trial for the "remaining consolidated cases" starting on a date that "will be determined." EX1101, 5. No party knows whether the '211 patent will be part of "the first of the consolidated cases" for trial starting on September 26, 2022 or part of the "remaining consolidated cases" starting on a later (unknown) date. *Id.* Any allegation to the contrary is pure speculation.

Factor 1 (Stay)—No party in the Related Litigation has requested a stay at this time. Huawei currently plans to seek a motion to stay after the Board's decision to institute IPR here because, in Judge Albright's court, a motion filed earlier would be premature. Again, the facts at play here are unique. There are six distinct lawsuits (asserting six unrelated patents) all unrealistically scheduled for trial on the same date. In such unique circumstances, it is unclear how Judge Albright would rule on a motion to stay for the particular lawsuit involving the '211 patent, especially after IPR is instituted against the '211 patent months before the due date for Patent Owner to amend its complaint (December 2021) and long before expert reports/discovery (March 2022). This cloud of uncertainty means Factor 1 is neutral.

Factor 2 (Trial Date)—While the Court set September 26, 2022 as a placeholder trial date for an unknown "first" subset of the six asserted patents and a later (unknown) trial for the "remaining consolidated cases," it is far from certain

whether the ’211 patent will be part of the “first” trial or the later second trial. EX1105, 5. The only certainty at this time is that several of the six patents will not be part of the September 26, 2022 trial because they will be grouped into the “remaining consolidated cases.” *Id.* Presently, there is no hint as to how the scheduling shuffle will play out, and it would be erroneous for any part to speculate that the ’211 patent will necessarily be excluded from the “remaining consolidated cases.” *Id.*

The *Fintiv* panel noted that the Board “generally take[s] courts’ trial schedules at face value absent some strong evidence to the contrary.” *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 15, 13 (PTAB, “informative,” May 13, 2020) (“*Fintiv II*”). For the reasons detailed above, such “strong evidence” exists on this record. Due to WSOU’s litigation tactics, neither the Court nor any party knows which one of the six asserted patents will be the subject of the trial starting on September 26, 2022. There is, in effect, no *certain* date for a jury trial that specifically addresses the ’211 patent.

The “informative” guidance in *Sand Revolution* aligns with the facts of this case. *Sand Revolution*, IPR2019-01393, Paper 24 at 8-10. Even if Patent Owner (improperly) speculates the district court will necessarily insert the ’211 patent into the “first” subset for a jury trial on September 26, 2022, the narrow gap in time between the jury’s final verdict (end of September 2022 or later) and the Board’s

projected Final Written Decision (October 2022) is less than one month. The panel in *Sand Revolution*, also facing meaningful questions of uncertainty about the trial date, weighed Factor 2 "marginally" *against* denial with a three-month time gap. *Id.* The *Sand Revolution* guidance demonstrates the proper result when the district court's "evolving schedule" makes it "unclear" when the trial would be held. *Id.* A similar lack of clarity exists in this case but for a slightly different reason—there is significant uncertainty as to whether the '211 patent will be in the "first" subset for trial on September 26, 2022 or in the second subset of the "remaining consolidated cases" for trial at a later unknown date. EX1101, 5.

Similarly, the Board's analysis in *Google LLC, et al. v. Parus Holdings, Inc.* is compelling. *See* IPR2020-00846, Paper 9, 12-14 (PTAB Oct. 21, 2020). There, the district court reserved a broad range of "predicted" trial dates but declined to specify further. *Id*. (noting a trial date range of July 12-30, 2021, and further noting the court's statement that it was "not going to pick a date right now"). With "only three months" between the range of trial dates and a final written decision, the Board deemed Factor 2 "neutral" based on "substantial uncertainty in the Texas court's 'Predicted Jury Selection/Trial' date." *Id*.

The less-than-a-month time gap presently at issue is narrower than *Sand Revolution* and the trial date uncertainty is comparable to *Google v. Parus*. The well-reasoned analysis in *Sand Revolution* weighed Factor 2 against discretionary

denial. A similar outcome is appropriate here.

Factor 3 (Investment)—The Related Litigation is currently in its infancy. Huawei has yet to serve its preliminary invalidity contentions, and the parties have yet to exchange proposed terms for construction. Huawei acted promptly in response to WSOU's identification of asserted claims in preliminary infringement contentions, filing this Petition only nine weeks after initially learning of the asserted claims and about six weeks after Huawei's in-house counsel was finally permitted to view the charts of the preliminary infringement contentions. *See* EX1101, 1.

At the projected date of institution (October 2021), the fact discovery period will have five more months of duration before the close of fact discovery (March 24, 2022), and expert reports/discovery will not even start until later (closing in May 19, 2022). EX1101, 4. Beyond a *Markman* order, which is not dispositive here and is unrelated to the invalidity issues based upon the prior art publications cited in this Petition, the Court will have not issued any substantive orders relevant to invalidity based on prior art publications.

The facts here compare favorably to *Fintiv*. In that case, also co-pending with litigation at the Western District of Texas, the petitioner filed *five months* after receiving preliminary infringement contentions, but the petition here was filed within nine weeks of receiving the asserted claim numbers (and just six weeks after Patent Owner authorized Huawei's in-house counsel to view the claim charts). *See*

Fintiv II at 9. There, "[a]t the time of filing the Petition, the parties were in the midst of preparations for the *Markman* hearing," while here, the parties have not even exchanged terms. *Id*.

The "informative" guidance in *Sand Revolution* is telling here too. By the time of institution in this proceeding, the Related Litigation will be at a similar posture where "aside from the district court's *Markman* Order, much of the district court's investment relates to ancillary matters untethered to the validity issue itself." *Sand Revolution*, IPR2019-01393, Paper 24, 10-11. The parallels are also notable because:

> [M]uch work remains in the district court case as it relates to invalidity: fact discovery is still ongoing, expert reports are not yet due, and substantive motion practice is yet to come.

Id. at 11 (internal citation omitted); *see also Fintiv I* at 10 ("If, at the time of the institution decision, the district court has not issued orders related to the patent at issue in the petition, this fact weighs against exercising discretion to deny institution").

In fact, the circumstances under Factor 3 here are similar to *Sotera*. *See Sotera Wireless, Inc. v. Masimo Corporation*, IPR2020-01019, Paper 12, 16-17 (PTAB Precedential Dec. 1, 2020) ("much other work remains in the parallel proceeding as it relates to invalidity" and the "explanation for timing of the Petition is reasonable,

… particular in view of the large number of patents and claims"). In this case too, Factor 3 "weighs in favor of not exercising discretion to deny" as a result of "the relatively limited investment in the parallel proceeding to date" and "the fact that the timing of the Petitioner was reasonable." *Id.* at 17.

Factor 4 (Overlap)— As an initial matter, no party currently knows whether the '211 patent will be part of the "remaining consolidated cases" for second trial starting on a later (unknown) date after the Board's final written decision here. EX1101, 5; *supra*, Analysis of Factors 1-2. In such circumstances, there would be absolutely no overlap between invalidity grounds addressed in the Board's final written decision and in the later jury trial because §315(e)(2) necessarily forbids it. Given the undefined nature of which one of the jury trials will actually include the '211 patent, these questions related to "overlap" in Factor 4 are, at best, speculative.

Moreover, even if Patent Owner indulges in speculation to assume that the '211 patent will necessarily be part of the "first" subset of cases for trial on September 26, 2022 rather than in the later subset, Huawei's stipulation here "mitigates" concerns related to overlapping prior art grounds. *Sand Revolution*, IPR2019-01393, Paper 24, 11-12; *see* EX1102 (not pursue "the same prior art grounds"). According to this informative guidance, Factor 4 weighs at least "marginally in favor not exercising discretion to deny IPR." *Sand Revolution*, IPR2019-01393, Paper 24, 12.

Factor 5 (Parties)—Because the parties here and at the District Court are the same, Factor 5 favors denial if trial precedes the Board's Final Written Decision and favors institution if the opposite is true (due to the 35 U.S.C. 315(e)(2) estoppel provision). *Google*, IPR2020-00846, Paper 9, 20-21 ("[W]e decline to speculate as to whether we are likely to address the challenged patent before the Texas court. Thus, [Factor 5] is neutral."). Neither circumstance can be confirmed in this case without improper speculation because the *actual* date of a jury trial involving the '211 patent is uncertain. EX1101, 5 (a later unknown trial for "the remaining consolidated cases"). Under these unique circumstances, Factor 5 is neutral.

Factor 6 (Merits and Other Circumstances)—The merits of this Petition are particularly strong as demonstrated in Grounds 1(A)-2(B). Moreover, WSOU—an entity specializing in patent licensing and negotiation—has asserted the '211 patent's overbroad claims against Huawei's Cloud Stack products. *See* EX1012. Fully vetting a fourteen-year-old patent (filed 2007) only now asserted against Huawei's product would be beneficial to the economy. *Consolidated Trial Practice Guide*, 56 (quoting 35 U.S.C. §316(b)). Factor 6 and the *Fintiv* Factors as a whole strongly favor institution.

Finally, Petitioner notes the ongoing legal challenge to discretionary denials of IPR based on the *Fintiv* and *NHK* precedential decisions (*e.g.*, *Apple Inc. et al. v. Iancu*, No. 5:20-cv-06128 (N.D. Cal.)), and reserves the opportunity to address the

result of that case and any impact in this proceeding.

IX. CONCLUSION

Petitioner requests IPR of the Challenged Claims pursuant to Grounds 1(A)-2(B).

Respectfully submitted,

Dated: April 6, 2021

/Nicholas W. Stephens/
Nicholas W. Stephens, Reg. No. 74,320

(Control No. IPR2021-00689)

Attorney for Petitioner

CERTIFICATION UNDER 37 CFR § 42.24

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 13,876 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Respectfully submitted,

Dated: April 6, 2021

/Nicholas W. Stephens/
Nicholas W. Stephens, Reg. No. 74,320

Attorney for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on April 6, 2021, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided via Federal Express, to the Patent Owner by serving the correspondence address of record as follows:

WSOU Investments, LLC
11150 Santa Monica Blvd., Suite 1400
Los Angeles, CA 90025

/Edward G. Faeth/
Edward Faeth
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(202) 626-6420